Abstract

Input picture data are encrypted with high secrecy and restoration against an error of encrypted data. An EXOR circuit 100 calculates input picture data and a pseudo random sequence and obtains encrypted data. The obtained encrypted data are held in an FF circuit 101. The FF circuit 101 is reset for each line. Counters 102 and 103 count for each line or each frame and are reset for each frame or at the beginning of a program. An encryption device 105 encrypts outputs of an FF circuit 104 that holds a fixed value, the counters 103 and 102, and the FF circuit 101 with a key (K) and generates a pseudo random sequence. A shift register 106 divides the bit sequence. The EXOR 100 calculates the output of the shift register 106 and the input picture data and obtains encrypted data. Since the encrypted output is fed back, data cannot be stolen using a successive input of the same data. In addition, since an encrypted output that is fed back is reset for each line, the encrypted output can be completely recovered from an error.